UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,193	10/16/2003	Ji Wei Lin	TS01-513	7561

42717 7590 07/24/2007

HAYNES AND BOONE, LLP
901 MAIN STREET, SUITE 3100
DALLAS, TX 75202

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
07/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/687,193	LIN ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8,9,13,14,16-23,26,27,31,32,34-41,44,45,49,50 and 52-54* is/are pending in the application.

4a) Of the above claim(s) *6,7,10-12,15,24,25,28-30,33,42,43,46-48 and 51* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8,9,13,14,16-23,26,27,31,32,34-41,44-45, 49-50 and 52-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the communication dated 5/8/2007 with the amendments to claims 1-5, 8-9, 13-14, 16-23, 26-27, 31-32, 34-41, 44-45, 49-50 and 52-54 and the cancellation of claims 6-7, 10-12, 15, 24-25, 28-30, 33, 42-43, 46-48 and 51.

2. Claims 1-5, 8-9, 13-14, 16-23, 26-27, 31-32, 34-41, 44-45, 49-50 and 52-54 are pending.

Response to Arguments

3. Applicant's arguments filed 5/8/2007 have been fully considered but they are not persuasive. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both references are directed to systems and methods for managing transaction data across a computer network (i.e. the Internet) (see Meffert: 0002 and Cox: 0001). As addressed in the previous office action, Cox discloses converting recipient's address from an email format to an internet format and vice versa (i.e. DNS server 206). Also as well known in the data communications world that the heart of how the Internet works is the domain

name server (DNS), the way in which computers contact each other and do things such as exchange e-mail or display Web pages. DNS translates "easy-to-remember" email format (e.g. username@abc.com) into "hard-to-remember" internet format (e.g. "123.45.67.89") and vice versa. It is obvious to combine the conversion process in Meffert system which is also dealing with information over the Internet to take advantage of the technology already existed such as DNS. Meffert does not teach against the combination as stated in the remark, Meffert discloses the advantages and disadvantages of several methods such as "Digital Rights Management" ("DRM"), "Electronic Data Interchange" ("EDI"), as well as "Pretty Good Privacy" ("PGP"), "Secure Socket Layer" ("SSL") and offers a more robust security and identity authentication for content delivering over the Internet.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 4-5, 8, 19, 22-23, 26, 37, 40-41, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170).

a) As to claim 1, Meffert discloses a method of integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email

(e.g. a secure content delivery system and method for implementing of public key infrastructure (PKI) based encryption and specifically to harnessing the advantages of PKI to provide encryption of and controlled access to data including email, email attachments, see Meffert: 0002) comprising: obtaining recipient's encryption software public key from an encryption software key server (i.e. local agent 130 requests and obtains the necessary keys from control server 200, see Meffert: 0076, a package of encrypted content is generated using PKI-based encryption by obtaining at least one public key from the control server, the encrypted package is sent to the control server, the control server transmits the package to the recipient local agent, the recipient local agent decrypts the encrypted content in the package, see Meffert: Abstract, it is understood that the necessary keys are the recipients' public keys used for encrypting, so then later the recipients' private keys are used for decrypting the encrypted content in the package); using said recipients' encryption software public key to encrypt an email (i.e. the email content is encrypted with the appropriate keys, see Meffert: 0076); using said recipients' encryption software public key to encrypt an attachment (i.e. the email and/or any attachments is encrypted using PKI cryptography, see Meffert: 0076). Meffert is silent on the capability of converting recipient's address from an email format to an Internet format and converting recipient's address from said Internet format to said email format. Cox is relied on for the teaching of converting recipient's address from an email format to an Internet format and converting recipient's address from said Internet format to said email format (i.e. domain name system (DNS) server 206 converts the standard e-mail format to a numeric Internet protocol (IP) format, see Cox: 0022). Cox

does not explicitly disclose converting said recipient's address from said internet format to said email format, however it is well known in the data communications world that the domain name server (DNS) translates domain names (e.g. email) to Internet Protocol address and vice versa. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of converting recipient's address from an email format to an Internet format and converting recipient's address from said Internet format to said email format in the system of Meffert, as Cox teaches, so as to make the system simply to use (see Meffert: 0010) by having DNS attachs easy-to-remember domain names (such as "username@postini.com") to hard-to-remember IP addresses (such as 123.45.67.89).

b) As to claim 4, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein converting the recipient's address from email format to internet format is required to obtain the encryption software public key (i.e. domain name system (DNS) server 206 converts the standard e-mail format to a numeric Internet protocol (IP) format, see Cox: 0022 and keys are obtained from the control server, see Meffert: 0076).

c) As to claim 5, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein said encryption software public key is obtained from an encryption software server (i.e. local agent 130 requests and obtains the necessary keys from control server 200, see Meffert: 0076).

d) As to claim 8, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein said recipient's address is converted from said internet format to email format to allow email processing using said email platform (i.e. the domain name server (DNS) translates domain names (e.g. email) to Internet Protocol address and vice versa to allow email processing, see Cox: 0022).

e) As to claim 19, this claim is directed to a hardware implementation of method of claim 1 and is rejected by a similar rationale applied against claim 1 above.

f) As to claim 22, this claim is directed to a hardware implementation of method of claim 4 and is rejected by a similar rationale applied against claim 4 above.

g) As to claim 23, this claim is directed to a hardware implementation of method of claim 5 and is rejected by a similar rationale applied against claim 5 above.

h) As to claim 26, this claim is directed to a hardware implementation of method of claim 8 and is rejected by a similar rationale applied against claim 8 above.

i) As to claim 37, this claim is directed to a software implementation of method of claim 1 and is rejected by a similar rationale applied against claim 1 above.

j) As to claim 40, this claim is directed to a software implementation of method of claim 4 and is rejected by a similar rationale applied against claim 4 above.

k) As to claim 41, this claim is directed to a software implementation of method of claim 5 and is rejected by a similar rationale applied against claim 5 above.

l) As to claim 44, this claim is directed to a software implementation of method of claim 8 and is rejected by a similar rationale applied against claim 8 above.

6. Claims 2-3, 13-14, 18, 20-21, 31-32, 36, 38-39, 49-50 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170) and further in view of applicant admitted prior art (AAPA).

a) As to claim 2, the combination of Meffert and Cox discloses the method of claim 1 further comprising: providing a means for a user to read an encrypted email and encrypted email attachment (i.e. local agent 130 launches a viewer within which the encrypted content including any attached files are decrypted and, thus, viewed, see Meffert: 0074), however it is silent of the capability of requesting a user to type a password of an encryption software private key. The applicant admitted prior art (AAPA) discloses requesting user to type a password of an encryption software private key (see AAPA: 0006). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of requesting user to type a password of an encryption software private key in the system of Meffert and Cox, as AAPA discloses, so as to provide robust security and identity authentication with respect to content delivered over the Internet (see Meffert: 0010).

b) As to claim 3, the combination of Meffert, Cox and AAPA teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 2 further comprising step of allowing users to use a familiar Email software interface to do encryption software key management (i.e. the present invention comprises two main components: a local agent, in conjunction with an application specific interface (ASI) and a control server, these two components can function independently or in combination to allow users to operate existing messaging

software applications, provide the necessary integration to employ PKI-based encryption using that messaging software application and to access application services functionality and PKI certificate and management processes, see Meffert: 0035).

c) As to claim 13, the combination of Meffert, Cox and AAPA discloses the method of claim 2 wherein said password and encryption software private key are used to decrypt said encrypted email (i.e. the typed in password is used to decrypt mail content, see AAPA: 0006 and private key in the public/private key pair is used for decrypt mail content, see Meffert: 0006).

d) As to claim 14, the combination of Meffert, Cox and AAPA discloses the method of claim 2 wherein said password and encryption software private key are used to decrypt said encrypted email attachment (i.e. the typed in password is used to decrypt attachment files, see AAPA: 0006 and private key in the public/private key pair is used for decrypt attachment files, see Meffert: 0006).

e) As to claim 18, the combination of Meffert, Cox and AAPA teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 3 wherein said encryption software key management includes sending out a user's encryption software public key to other people (i.e. the electronic delivering statements or bills with component 550 to receive account, public key and certificate data corresponding to each client associated with the billing data, the client billing data and account and certificate data are then packaged together and passed to the high volume encryption component which employs PKI based encryption using the certificate packaged with the billing data and account data, it is understood

that the public keys are distributed to other people such as the presentment services, see Meffert: 0095-0096).

f) As to claim 20, this claim is directed to a hardware implementation of method of claim 2 and is rejected by a similar rationale applied against claim 2 above.

g) As to claim 21, this claim is directed to a hardware implementation of method of claim 3 and is rejected by a similar rationale applied against claim 3 above.

h) As to claim 31, as suggested depending on claim 30, this claim is directed to a hardware implementation of method of claim 13 and is rejected by a similar rationale applied against claim 13 above.

i) As to claim 32, as suggested depending on claim 30, this claim is directed to a hardware implementation of method of claim 14 and is rejected by a similar rationale applied against claim 14 above.

j) As to claim 36, as suggested depending on claim 21, this claim is directed to a hardware implementation of method of claim 18 and is rejected by a similar rationale applied against claim 18 above.

k) As to claim 38, this claim is directed to a software implementation of method of claim 2 and is rejected by a similar rationale applied against claim 2 above.

l) As to claim 39, this claim is directed to a software implementation of method of claim 3 and is rejected by a similar rationale applied against claim 3 above.

m) As to claim 49, as suggested depending on claim 48, this claim is directed to a software implementation of method of claim 13 and is rejected by a similar rationale applied against claim 13 above.

n) As to claim 50, as suggested depending on claim 48, this claim is directed to a software implementation of method of claim 14 and is rejected by a similar rationale applied against claim 14 above.

o) As to claim 54, as suggested depending on claim 39, this claim is directed to a software implementation of method of claim 18 and is rejected by a similar rationale applied against claim 18 above.

7. Claims 9, 27 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170) and further in view of Wolf et al. (5,818,447).

a) As to claim 9, the combination of Meffert and Cox discloses the method of claim 1, particularly converting recipient's address from said internet format back to rmail format (see Cox: 0022), however it is silent on the capability of having conversion allows retention of rich text content. Wolf is relied on for the teaching of having conversion of said recipient's address from said internet format back to email format allows retention of rich text content (i.e. Wolf discloses a system and method for handling email, see Wolf: col. 1, lines 6-10, Wolf acknowledges rich text capabilities in the email program, see Wolf: col. 1, lines 36-37, and discloses a system that provide sophisticated formatting and editing options in the context of email environment that is compatible with downlevel (rich text) email clients, see Wolf: col. 2, lines 2-5, in particular, the MAPI formats ensures the interoperability between an embodiment of the present invention, a prior art rich text mail client and other mail clients and gateways,

see Wolf: col. 16, lines 29-32). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having conversion of said recipient's address from said internet format back to email format allows retention of rich text content in the system of Meffert and Cox, as Wolf teaches, so as to provide a system for creating sophisticated documents for transmission via electronic email (see Wolf: col. 1, line 67 to col. 2, line 1).

b) As to claim 27, this claim is directed to a hardware implementation of method of claim 9 and is rejected by a similar rationale applied against claim 9 above.

c) As to claim 45, this claim is directed to a software implementation of method of claim 9 and is rejected by a similar rationale applied against claim 9 above.

8. Claims 16, 34 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170) in view of applicant admitted prior art (AAPA) and further in view of Goldstone (2003/0142364).

a) As to claim 16, the combination of Meffert, Cox and AAPA discloses the method of claim 3, however it is silent on the capability of having encryption software key management includes changing password of an encryption software private key. Goldstone is relied on for the teaching of having encryption software key management includes changing password of an encryption software private key (i.e. the key pair could be changed frequently and the password required to access the private key could also be changed even more frequently, see Goldstone: 0052). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of

having encryption software key management includes changing password of an encryption software private key in the system of Meffert, Cox and AAPA, as Goldstone teaches, so as to provide robust security and identity authentication with respect to content delivered over the Internet (see Meffert: 0010).

b) As to claim 34, as suggested depending on claim 21, this claim is directed to a hardware implementation of method of claim 16 and is rejected by a similar rationale applied against claim 16 above.

c) As to claim 52, as suggested depending on claim 37, this claim is directed to a software implementation of method of claim 16 and is rejected by a similar rationale applied against claim 16 above.

9. Claims 17, 35 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002//0059144) in view of Cox et al. (2005/0044170) in view of applicant admitted prior art (AAPA) and further in view of Smith et al. (6,651,166).

a) As to claim 17, as suggested depending on claim 3, the combination of Meffert, Cox and AAPA discloses the method of claim 3, however it is silent on the capability of having encryption software key management includes registering other encryption software public keys with said encryption software key server. Smith is relied on for the teaching of having encryption software key management includes registering other encryption software public keys with said encryption software key server (i.e. register public key with a trusted authority, see Smith: col. 2, lines 33-35). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the

use of having encryption software key management includes registering other encryption software public keys with said encryption software key server in the system of Meffert, Cox and AAPA, as Smith discloses, so as to securely deliver electronic documents to remote recipients (see Smith: col. 1, lines 5-10).

b) As to claim 35, as suggested depending on claim 21, this claim is directed to a hardware implementation of method of claim 17 and is rejected by a similar rationale applied against claim 17 above.

c) As to claim 53, as suggested depending on claim 37, this claim is directed to a software implementation of method of claim 17 and is rejected by a similar rationale applied against claim 17 above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
7/17/07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER